Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - 1Two Livre d'Or Input Validation Errors Permit Cross-Site Scripting
  - APG Technology ClassMaster Folder Access Vulnerability
  - bttlxeForum Discloses Installation Path to Remote Users
  - Darrel O'Neil ASP Virtual News Remote SQL Injection Vulnerability
  - DotNetNuke Script Insertion Vulnerabilities
  - Fastream NETFile FTP/Web Server FTP Bounce Vulnerability
  - GASoft Gurgens Guest Book Discloses Database and Passwords to Remote Users
  - GASoft Ultimate Forum Discloses Database and Passwords to Remote Users
  - GeoVision Digital Video Surveillance System Authentication Bypass
  - Keyvan1 ImageGallery Information Disclosure Vulnerability
  - EnCase Device Configuration Overlay Data Acquisition Vulnerability
  - MaxWebPortal Cross-Site Scripting and SQL Injection
  - **Microsoft Media Player & Windows/MSN Messenger PNG Processing (Updated)**
  - Microsoft IPV6 TCPIP Loopback LAND Denial of Service Vulnerability
  - **Microsoft MSN Messenger Remote Code Execution Vulnerability (Updated)**
  - Microsoft Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities (Updated)
  - Microsoft Windows Media Player May Allow Redirection
  - **Microsoft Word Remote Code Execution and Escalation of Privilege Vulnerabilities (Updated)**
  - Mozilla Firefox Download Dialog Spoofing Vulnerabilities
  - **RSA Authentication Agent for Web Buffer Overflow Vulnerability (Updated)**
  - Sigma ISP Manager SQL Injection Vulnerabilities
  - **Software602 602LAN SUITE Local File Detection and Denial of Service (Updated)**
  - Woppoware PostMaster Multiple Vulnerabilities
  - WSW ShowOff! Digital Media Software Two Vulnerabilities
  - Yahoo! Messenger URL Handler Remote Denial Of Service Vulnerability
- UNIX / Linux Operating Systems
  - **Apple Mac OS X Multiple Vulnerabilities (Updated)**
  - **Apple Mac OS X NetInfo Setup Tool Buffer Overflow (Updated)**
  - Apple QuickTime Quartz Composer File Information Disclosure
  - bzip2 Remote Denial of Service
  - **BZip2 File Permission Modification (Updated)**
  - **Carnegie Mellon University Cyrus IMAP Server Multiple Remote Buffer Overflows (Updated)**
  - Cheetah Elevated Privileges
  - **Ethereal Multiple Remote Protocol Dissector Vulnerabilities (Updated)**
  - FreeBSD Hyper-Threading Technology Support Information Disclosure
  - **FreeRadius 'rlm_sql.c' SQL Injection & Buffer Overflow (Updated)**
  - **GNU GZip Directory Traversal (Updated)**
  - **GnuTLS Padding Validation Remote Denial of Service (Updated)**
  - **GNU Vim / Gvim Modelines Command Execution Vulnerabilities (Updated)**
  - Gzip Zgrep Arbitrary Command Execution
  - HT Editor ELF & PE Parser Remote Code Execution
  - **KDE DCOPServer Local Denial of Service (Updated)**
  - **KDE 'DCOPIDLING' Library (Updated)**
  - **KDE Kommander Remote Arbitrary Code Execution (Updated)**
  - **LBL TCPDump Remote Denials of Service (Updated)**
  - Mozilla Bugzilla Information Disclosure
  - **Multiple Vendors Apache 'HTDigest' Buffer Overflow (Updated)**
  - **Multiple Vendors KDE 'kimgio' image library Remote Buffer Overflow (Updated)**
  - **Multiple Vendors GDK-Pixbuf BMP Image Processing Double Free Remote Denial of Service (Updated)**
  - Multiple Vendors Linux Kernel ELF Core Dump Buffer Overflow
  - Multiple Vendor Linux Kernel pktcdvd & raw device Block Device
  - **Multiple Vendors NASM error() Buffer Overflow (Updated)**
  - **Multiple Vendors Gaim Jabber File Request Remote Denial of Service (Updated)**
  - **Multiple Vendors Gaim 'Gaim_Markup_Strip_HTML()' Function Remote Denial of Service (Updated)**

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
1Two.org 1Two Livre d'Or 1.0	An input validation vulnerability has been reported that could let a remote malicious user conduct Cross-Site Scripting attacks. The 'guestbook.php' script does not properly validate user-supplied input in the nom, email, and message fields. The vendor has reportedly issued a fix. Currently we are not aware of any exploits for this vulnerability.	1Two Livre d'Or Input Validation Errors Permit Cross-Site Scripting CAN-2005-1644	High	Security Tracker Alert ID: 1013971, May 13, 2005
APG Technology ClassMaster	A vulnerability has been reported that could let remote malicious users gain unauthorized access to users' folders. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	APG Technology ClassMaster Folder Access Vulnerability CAN-2005-1577	High	Security Focus, Bugtraq ID 13604, May 12, 2005
Battleaxe Software bttlxeForum 2.0	A vulnerability has been reported that could let a remote malicious user determine the installation path and other system information by supplying a URL containing a scripting code in hex format. No workaround or patch available at time of publishing. An exploit has been published.	bttlxeForum Discloses Installation Path to Remote Users CAN-2005-1570	Medium	Security Tracker Alert ID: 1013934, May 11, 2005
Darrel O'Neil ASP Virtual News Manager	A vulnerability has been reported that could let a remote malicious user inject SQL commands. This is due to an input validation error in the 'aspvirtualnews/admin_login.asp' script with the 'password' parameter. No workaround or patch available at time of publishing. An exploit has been published.	Darrel O'Neil ASP Virtual News Remote SQL Injection Vulnerability CAN-2005-1573	High	Security Tracker Alert ID: 1013933, May 11, 2005
DotNetNuke DotNetNuke 3.0.12	Multiple vulnerabilities exist that could let remote malicious users conduct script insertion attacks. Input passed to the 'User-Agent' HTTP header, the username, and certain registration data is not properly validated. Update to version 3.0.12. There is no exploit code required.	DotNetNuke Script Insertion Vulnerabilities CAN-2005-0040	High	Secunia SA15397, May 17, 2005
Fastream Technologies Fastream NETFile FTP/Web Server 7.4.6	A vulnerability has been reported that could let remote malicious users bypass certain security restrictions or cause a Denial of Service. This is caused due to missing validation of the IP address specified as argument to the PORT command and can be exploited via so-called 'FTP Bounce' attacks to open connections to arbitrary systems via the FTP server. Update to version 7.6 and disable FXP support. Currently we are not aware of any exploits for this vulnerability.	Fastream NETFile FTP/Web Server FTP Bounce Vulnerability CAN-2005-1646	Medium	SIG^2 Vulnerability Research Advisory, May 17, 2005
GASoft Gurgens Guest Book 2.1	A vulnerability has been reported in Gurgens Guest Book that could let a remote malicious user access the 'Genid.dat' file in the 'db' directory and then decrypt the passwords in the file. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GASoft Gurgens Guest Book Discloses Database & Passwords to Remote Users CAN-2005-1647	Medium	Security Tracker Alert ID: 1013976, May 16, 2005
GASoft Ultimate Forum 1.0	A vulnerability has been reported that could let a remote malicious user access the 'Genid.dat' file in the 'db' directory and then decrypt the passwords in the file. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GASoft Ultimate Forum Discloses Database and Passwords to Remote Users CAN-2005-1648	Medium	Security Tracker Alert ID: 1013974, May 16, 2005
GeoVision Digital Video Surveillance System 6.04, 6.1, and 7.0	A vulnerability has been reported that could let a remote malicious user view sensitive information. This is because images can be accessed directly via the JPEG Image Viewer. Enable the "Enhanced Network Security" feature introduced in version 7.0. Currently we are not aware of any exploits for this vulnerability.	GeoVision Digital Video Surveillance System Authentication Bypass CAN-2005-1552 CAN-2005-1553	Medium	Esqo Security Advisory , May 10, 2005

Guidance Software EnCase Forensic Edition 4.18a	A vulnerability has been reported that could let a remote malicious user hide information on a disk. Support is missing for Device Configuration Overlays (DCO) and the program fails to read parts of a disk using this feature. No workaround or patch available at time of publishing. There is no exploit code required.	Guidance Software EnCase Device Configuration Overlay Data Acquisition Vulnerability CAN-2005-1578	Medium	Secunia SA15340, May 13, 2005
Keyvan1 ImageGallery	A vulnerability have been reported that could let a remote malicious user download the database and access the administrative password. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Keyvan1 ImageGallery Information Disclosure Vulnerability CAN-2005-1645	High	Security Tracker Alert ID: 1013970, May 13, 2005
MaxWebPortal 1.x	Multiple vulnerabilities have been reported that could let a remote malicious user conduct Cross-Site Scripting and SQL injection attacks. These are due to input validation errors in the 'mod,' 'M,' and 'type' parameters in 'post.asp' and 'Forum_Title' parameter in 'post.asp,' the 'txtAddress,' 'message' and 'subject' parameters in 'post_info.asp,' the 'andor' parameter in 'search.asp,' the 'verkey' parameter in 'pop_profile.asp,' a certain password parameter in 'pop_profile.asp,' and the 'Remove' and 'Delete' parameters in 'pm_delete2.asp.' No workaround or patch available at time of publishing. Exploits have been published.	MaxWebPortal Cross-Site Scripting & SQL Injection CAN-2005-1561 CAN-2005-1562	High	Zinho's Security Advisory, May 11, 2005
Microsoft Windows Media Player 9 Series, Windows Messenger 5.0, MSN Messenger 6.1, 6.2	Several vulnerabilities exist: a vulnerability exists in Media Player due to a failure to properly handle PNG files that contain excessive width or height values, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the Windows and MSN Messenger due to a failure to properly handle corrupt or malformed PNG files, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-009.mspx V1.1: Bulletin updated with information on the mandatory upgrade of vulnerable MSN Messenger clients in the caveat section, as well as changes to the Workarounds for PNG Processing Vulnerability in MSN Messenger. V1.2: Bulletin updated with correct file version information for Windows Messenger 5.0 update, as well as added Windows Messenger 5.1 to "Non-Affected Software" list. V2.0: The update for Windows Messenger version 4.7.0.2009 (when running on Windows XP Service Pack 1) was failing to install when distributed via SMS or AutoUpdate. An updated package corrects this behavior. **V2.1: Bulletin updated to update the "Security Update Information" section for the Microsoft Windows Messenger 4.7.0.2009 (when running on Windows XP Service Pack 1) security update.** An exploit script has been published for MSN Messenger/Windows Messenger PNG Buffer Overflow vulnerability.	Microsoft Media Player & Windows/MSN Messenger PNG Processing CAN-2004-1244 CAN-2004-0597	High	Microsoft Security Bulletin, MS05-009, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#259890 Security Focus, February 10, 2005 Microsoft Security Bulletin MS05-009 V1.1, February 11, 2005 Microsoft Security Bulletin, MS05-009 V1.2, February 15, 2005 Microsoft Security Bulletin, MS05-009 V2.0, April 12, 2005 **Microsoft Security Bulletin, MS05-009 V2.1, May 11, 2005**
Microsoft Windows XP Service Pack 2, Windows 2003 Server Service Pack 1	A remote Denial of Service vulnerability has been reported. The IPV6 TCP/IP stack is prone to a 'loopback' condition initiated by sending a TCP packet with the 'SYN' flag set and the source address and port spoofed to equal the destination source and port. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft IPV6 TCPIP Loopback LAND Denial of Service Vulnerability CAN-2005-1649	Low	Security Focus Bugtraq ID 13658, May 17, 2005
Microsoft MSN Messenger 6.2	A vulnerability has been reported because MSN Messenger may not process a malformed GIF image with an improper height and width. This could let remote malicious users execute arbitrary code. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-022.mspx **V1.1: Bulletin updated with correct file version information for MSN Messenger 6.2.** Currently we are not aware of any exploits for this vulnerability.	Microsoft MSN Messenger Remote Code Execution Vulnerability CAN-2005-0562	High	Microsoft Security Bulletin MS05-022, April 12, 2005 Technical Cyber Security Alert TA05-102A US-CERT VU#633446 **Microsoft Security Bulletin MS05-022, May 11, 2005**

Microsoft Windows 2000 SP 3 and SP4 Windows XP SP 1 and SP2 Windows XP 64-Bit Edition SP1 and 2003 (Itanium) Windows Server 2003 Windows Server 2003 for Itanium-based Systems Windows 98, Windows 98 SE, and Windows ME	Multiple vulnerabilities have been reported that include IP Validation, ICMP Connection Reset, ICMP Path MTU, TCP Connection Reset, and Spoofed Connection Request. These vulnerabilities could let remote malicious users execute arbitrary code or execute a Denial of Service. Updates available: http://www.microsoft.com/technet/security/bulletin/MS05-019.mspx **V1.1: Bulletin updated to advise customers that Microsoft plans to re-release the MS05-019 security update in June, 2005. Until the re-release of this security update is available, customers experiencing the symptoms described in Microsoft Knowledge Base Article 898060 should follow the documented instructions to address this issue. If you are not experiencing this network connectivity issue Microsoft recommends that you install the currently available security update** A Proof of Concept exploit has been published.	Microsoft Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities CAN-2005-0048 CAN-2004-0790 CAN-2004-1060 CAN-2004-0230 CAN-2005-0688	Low/ High (High if arbitrary code can be executed)	Microsoft Security Bulletin MS05-019, April 12, 2005 Technical Cyber Security Alert TA05-102A US-CERT VU#233754 US-CERT VU#396645 **Microsoft Security Bulletin MS05-019, May 11, 2005**
Microsoft Windows Media Player 9 prior to 9.0.0.3263 and 10 prior to 10.0.0.3901	A vulnerability has been reported that could let a remote malicious user redirect the target user's player to an arbitrary web site. Certain types of Windows Media Digital Rights Management (WMDRM)-protected content can cause the target user's Windows Media Player to redirect to a specified web page. This may occur even if the target user's player has the 'Acquire licenses automatically for protected content' checkbox de-selected under the privacy options. The following updates are available: Windows Media Player 10: http://download.microsoft.com/download/9/9/c/99c6e0be-19ec-4ffd-b44a-c9b8f2886200/windowsmedia10-k b892313-x86-intl.exe Windows Media Player 9 Series for Windows 2000, Windows XP, and Windows Server 2003: http://download.microsoft.com/download/8/c/b/8cb07a83-3b1c - 4a95-a1c7-4e788c113829/windowsmedia9-kb892313-x86-intl.exe Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Media Player May Allow Redirection CAN-2005-1574	High	Microsoft Security Advisory (892313), May 10, 2005
Microsoft Word 2000, 2002 Works Suite 2001, 2002, 2003, and 2004 Office Word 2003	A buffer overflow vulnerability has been reported that could lead to remote execution of arbitrary code or escalation of privilege. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-023.mspx V1.1 Bulletin updated to point to the correct Exchange 2000 Server Post-Service Pack 3 (SP3) Update Rollup and to advise on the scope and caveats of workaround "Unregister xlsasink.dll and fallback to Active Directory for distribution of route information." **V1.2: Bulletin updated to add msiexec in the administrative installation in "Administrative Deployment" section for all versions.** Currently we are not aware of any exploits for this vulnerability.	Microsoft Word Remote Code Execution & Escalation of Privilege Vulnerabilities CAN-2004-0963 CAN-2005-0558	High	Microsoft Security Bulletin MS05-023, April 12, 2005 US-CERT VU#442567 US-CERT VU#752591 Microsoft Security Bulletin MS05-023 V1.1, April 14, 2005 **Microsoft Security Bulletin MS05-023 V1.2, May 11, 2005**
Mozilla Firefox 0.10.1 and 1.0 for Windows	Two vulnerabilities have been reported that could let remote malicious users to spoof file types in the file download dialog. Input validation errors occur in the filename and the 'Content-Type' header before being displayed in the file download dialog. The 'Content-Type' header is used for associating a file to a file type in the file download dialog, but the file extension is left intact when saving the file to disk with 'Save to Disk.' This can be exploited to spoof file types in the file download dialog. The vulnerabilities have been partially fixed in version 1.0.1. Currently we are not aware of any exploits for these vulnerabilities.	Mozilla Firefox Download Dialog Spoofing Vulnerabilities CAN-2005-1575 CAN-2005-1576	Medium	Secunia SA12979, May 12, 2005
RSA RSA Authentication Agent for Web for IIS 5, 5.2, 5.3	A vulnerability has been reported that could let remote malicious users execute arbitrary code. The is due to a boundary error and can cause a heap-based buffer overflow by sending an overly long piece of data via the chunked-encoding mechanism. A patch is available: https://knowledge.rsasecurity.com/ Currently we are not aware of any exploits for this vulnerability.	RSA Authentication Agent for Web Buffer Overflow Vulnerability CAN-2005-1471	High	Secunia, SA15222 , May 9, 2005 **US-CERT VU#790533**

Sigma ISP Manager 6.6 and prior	Multiple vulnerabilities have been reported that could let remote malicious users conduct SQL injection attacks. This is due to input validation errors in input passed to the 'username,' 'password,' and 'domain' fields in 'sigmaweb.dll.' No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Sigma ISP Manager SQL Injection Vulnerabilities CAN-2005-1639	High	Secunia SA15379, May 17, 2005
Software602 602LAN SUITE 2004.0.05.0413	A vulnerability has been reported that could let remote users detect the presence of local files and cause a Denial of Service. No redirection occurs when accessing the "mail" script with the "A" parameter referencing a valid local file via directory traversal attacks. **Upgrade available at:** **http://www.software602.com/download/** A Proof of Concept exploit has been published.	Software602 602LAN SUITE Local File Detection and Denial of Service CAN-2005-1423	Low	Secunia Advisory, SA15231, May 3, 2005 **Security Focus, 13519, May 11, 2005**
Woppoware PostMaster version 4.2.2 (build 3.2.5)	Multiple vulnerabilities have been reported that could let a remote malicious user detect the presence of local files, enumerate usernames, conduct Cross-Site Scripting attacks, and bypass certain security restrictions. These are due to errors in the web mail service, in the handling of the 'wmm' parameter in 'message.htm,' in the authentication process, and in validating the 'email' parameter in 'message.htm.' No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Woppoware PostMaster Multiple Vulnerabilities CAN-2005-1650 CAN-2005-1651 CAN-2005-1652 CAN-2005-1653	High	Secunia SA15268, May 11, 2005
WSW ShowOff! Digital Media Software 1.5.4	Two vulnerabilities have been reported that could let a remote malicious user cause a Denial of Service and view sensitive information. These are due to an input validation error in the request handling and an error in the communication handling. No workaround or patch available at time of publishing. An exploit has been published.	WSW ShowOff! Digital Media Software Two Vulnerabilities CAN-2005-1571 CAN-2005-1572	Medium	Secunia SA15300, May 11, 2005
Yahoo! Yahoo! Messenger 5.x to 6.0 Windows	A vulnerability has been reported that could let a remote malicious user cause a Denial of Service. This is because the application fails to properly handle exceptional conditions. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Yahoo! Messenger URL Handler Remote Denial Of Service Vulnerability CAN-2005-1618	Low	Security Focus Bugtraq ID 13626, May 13, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Apple Mac OS X 10.3-10.3.9, Mac OS X Server 10.3-10.3.9	Multiple vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'htdigest' due to a boundary error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in the AppKit component when processing TIFF files, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability was reported in the AppKit component when parsing certain TIFF images because an invalid call is made to the 'NXSeek()' function; a vulnerability was reported due to an error when handling AppleScript because code is displayed that is different than the code that is actually run, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to an error in the Bluetooth support because files are shared without notifying the user properly, which could let a remote malicious user obtain sensitive information; a Directory Traversal vulnerability was reported in the Bluetooth file, which could let a remote malicious user obtain sensitive information; a vulnerability was reported in the 'chfn,' 'chpass,' and 'chsh' utilities because certain external helper programs are invoked insecurely, which could let a malicious user obtain elevated privileges; a vulnerability was reported in Finder due to the insecure creation of '.DS_Store' files, which could let a malicious user obtain elevated privileges; a vulnerability was reported in Help Viewer because a remote malicious user can run JavaScript without imposed security restrictions; a vulnerability was reported in the LDAP functionality because passwords are stored in plaintext, which could let a remote malicious user obtain sensitive information; a vulnerability was reported due to errors when parsing XPM files, which could let a remote malicious user compromise the system; a vulnerability was reported in 'lukemftpd' because chroot restrictions can be bypassed, which could let a remote malicious user bypass restrictions; a vulnerability was reported in the Netinfo Setup Tool (NeST) when processing input passed to the ' -target' command line parameter due to a boundary error, which could let a malicious user execute arbitrary code; a vulnerability was reported when the HTTP proxy service in Server Admin is enabled because by default it is possible for everyone to use the proxy service; a vulnerability was reported in the HTTP proxy service in Server Admin for Mac OS X due to insufficient access restrictions, which could let a remote malicious user obtain unauthorized access; a vulnerability was reported in sudo in the environment clearing, which could let a malicious user obtain elevated privileges; a	Apple Mac OS X Multiple Vulnerabilities CAN-2004-0687 CAN-2004-0688 CAN-2004-1051 CAN-2004-1307 CAN-2004-1308 CAN-2005-0342 CAN-2005-1271 CAN-2005-1330 CAN-2005-1331 CAN-2005-1332 CAN-2005-1333 CAN-2005-1335 CAN-2005-1336 CAN-2005-1337 CAN-2005-1340 CAN-2005-1341 CAN-2005-1342 CAN-2005-1343 CAN-2005-1344	Low/ Medium/ High (Low if a DoS; Medium is sensitive information or elevated privileges can be obtained; and High if arbitrary code can be executed)	Apple Security Update, APPLE-SA-2005-05-03, May 3, 2005 US-CERT VU#140470 US-CERT VU#145486 US-CERT VU#258390 US-CERT VU#356070 **US-CERT VU#582934** **US-CERT VU#331694** **US-CERT VU#706838** **Technical Cyber Security Alert TA05-136A**

	vulnerability was reported in the Terminal utility, which could let a remote malicious user inject arbitrary data; a vulnerability was reported due to an error in the Terminal utility, which could let a remote malicious user inject commands in x-man-path URIs; and a vulnerability was reported in vpnd due to a boundary error, which could let a malicious user execute arbitrary code. Upgrades available at: http://www.apple.com/support/downloads/securityupdate2005005client.html http://www.apple.com/support/downloads/securityupdate2005005server.html Proofs of Concept exploits have been published.			
Apple Mac OS X Server 10.3-10.3.9	A buffer overflow vulnerability has been reported in the NetInfo Setup Tool (NeST) when excessive string values are processed through a command line parameter, which could let a malicious user execute arbitrary code with root privileges. Updates available at: http://www.apple.com/support/downloads/ Currently we are not aware of any exploits for this vulnerability.	Apple Mac OS X NetInfo Setup Tool Buffer Overflow CAN-2005-0594	High	Apple Security Update, APPLE-SA-2005-05-03, May 3, 2005 **US-CERT VU#354486**
Apple QuickTime Player 7.0	A vulnerability has been reported in the QuickTime Web plugin because Quartz Composer compositions that are embedded in '.mov' files can access system information, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Apple QuickTime Quartz Composer File Information Disclosure CAN-2005-1579	Medium	Security Tracker Alert, 1013961, May 12, 2005
bzip2 bzip2 1.0.2	A remote Denial of Service vulnerability has been reported when the application processes malformed archives. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/b/bzip2/ Currently we are not aware of any exploits for this vulnerability.	bzip2 Remote Denial of Service CAN-2005-1260	Low	Ubuntu Security Notice, USN-127-1, May 17, 2005
bzip2 bzip2 1.0.2 & prior	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions of target files. **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/b/bzip2/** There is no exploit code required.	BZip2 File Permission Modification CAN-2005-0953	Medium	Security Focus, 12954, March 31, 2005 **Ubuntu Security Notice, USN-127-1, May 17, 2005**
Carnegie Mellon University Cyrus IMAP Server 2.x	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in mailbox handling due to an off-by-one boundary error, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the imapd annotate extension due to an off-by-one boundary error, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in 'fetchnews,' which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exist because remote administrative users can exploit the backend; and a buffer overflow vulnerability exists in imapd due to a boundary error, which could let a remote malicious user execute arbitrary code. Update available at: http://ftp.andrew.cmu.edu/pub/cyrus/cyrus-imapd-2.2.11.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200502-29.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cyrus21-imapd/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html	Cyrus IMAP Server Multiple Remote Buffer Overflows CAN-2005-0546	High	Secunia Advisory, SA14383, February 24, 2005 Gentoo Linux Security Advisory, GLSA 200502-29, February 23, 2005 SUSE Security Announcement, SUSE-SA:2005:009, February 24, 2005 Ubuntu Security Notice USN-87-1, February 28, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:051, March 4, 2005 Conectiva Linux Security Announcement, CLA-2005:937, March 17, 2005 ALTLinux Security Advisory, March 29, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.005, April 5, 2005

	OpenPKG: ftp://ftp.openpkg.org/release/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-408.html** Currently we are not aware of any exploits for these vulnerabilities.			Fedora Update Notification, FEDORA-2005-339, April 27, 2005 **RedHat Security Advisory, RHSA-2005:408-04, May 17, 2005**
Cheetah Cheetah 0.9.16 a1	A vulnerability has been reported because modules are imported from the '/tmp' directory before searching for the path from the 'PYTHONPATH' variable, which could let a malicious user obtain elevated privileges. Upgrades available at: http://prdownloads.sourceforge.net/cheetahtemplate/Cheetah-0.9.17rc1.tar.gz?download There is no exploit code required.	Cheetah Elevated Privileges CAN-2005-1632	Medium	Secunia Advisory, SA15386, May 17, 2005
Ethereal Group Ethereal 0.8.14, 0.8.15, 0.8.18, 0.8.19, 0.9-0.9.16, 0.10-0.10.9	Multiple vulnerabilities were reported that affects more 50 different dissectors, which could let a remote malicious user cause a Denial of Service, enter an endless loop, or execute arbitrary code. The following dissectors are affected: 802.3 Slow, AIM, ANSI A, BER, Bittorrent, CMIP, CMP, CMS, CRMF, DHCP, DICOM, DISTCC, DLSw, E IGRP, ESS, FCELS, Fibre Channel, GSM, GSM MAP, H.245, IAX2, ICEP, ISIS, ISUP, KINK, L2TP, LDAP, LMP, MEGACO, MGCP, MRDISC, NCP, NDPS, NTLMSSP, OCSP, PKIX Qualified, PKIX1Explitit, Presentation, Q.931, RADIUS, RPC, RSVP, SIP, SMB, SMB Mailslot, SMB NETLOGON, SMB PIPE, SRVLOC, TCAP, Telnet, TZSP, WSP, and X.509. Upgrades available at: http://www.ethereal.com/distribution/ethereal-0.10.11.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200505-03.xml **Mandriva:** **http://www.mandriva.com/security/advisories** An exploit script has been published.	Ethereal Multiple Remote Protocol Dissector Vulnerabilities CAN-2005-1456 CAN-2005-1457 CAN-2005-1458 CAN-2005-1459 CAN-2005-1460 CAN-2005-1461 CAN-2005-1462 CAN-2005-1463 CAN-2005-1464 CAN-2005-1465 CAN-2005-1466 CAN-2005-1467 CAN-2005-1468 CAN-2005-1469 CAN-2005-1470	Low/ High (High if arbitrary code can be executed)	Ethereal Security Advisory, enpa-sa-00019, May 4, 2005 Gentoo Linux Security Advisory, GLSA 200505-03, May 6, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:083, May 11, 2005**
FreeBSD FreeBSD 5.4 & prior	A vulnerability was reported in FreeBSD when using Hyper-Threading Technology due to a design error, which could let a malicious user obtain sensitive information and possibly elevated privileges. Patches and updates available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:09.htt.asc Currently we are not aware of any exploits for this vulnerability.	FreeBSD Hyper-Threading Technology Support Information Disclosure CAN-2005-0109	Medium	FreeBSD Security Advisory, FreeBSD-SA-05:09, May 13, 2005
FreeRADIUS Server Project FreeRADIUS 1.0.2	Two vulnerabilities have been reported: a vulnerability was reported in the 'radius_xlat()' function call due to insufficient validation, which could let a remote malicious user execute arbitrary SQL code; and a buffer overflow vulnerability was reported in the 'sql_escape_func()' function, which could let a remote malicious user execute arbitrary code. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-13.xml** There is no exploit code required.	FreeRadius 'rlm_sql.c' SQL Injection & Buffer Overflow CAN-2005-1454 CAN-2005-1455	High	Security Tracker Alert ID: 1013909, May 6, 2005 **Gentoo Linux Security Advisory, GLSA 200505-13, May 17, 2005**

GNU gzip 1.2.4 a, 1.2.4, 1.3.3-1.3.5	A Directory Traversal vulnerability has been reported due to an input validation error when using 'gunzip' to extract a file with the '-N' flag, which could let a remote malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gzip/ Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-05.xml **IPCop:** **http://ipcop.org/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=3&orderby=dateD** A Proof of Concept exploit has been published.	GNU GZip Directory Traversal CAN-2005-1228	Medium	Bugtraq, 396397, April 20, 2005 Ubuntu Security Notice, USN-116-1, May 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 **Security Focus,13290, May 11, 2005**
GnuTLS GnuTLS 1.2 prior to 1.2.3; 1.0 prior to 1.0.25	A remote Denial of Service vulnerability has been reported due to insufficient validation of padding bytes in 'lib/gnutils_cipher.c.' Updates available at: http://www.gnu.org/software/gnutls/download.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-04.xml **Mandriva:** **http://www.mandriva.com/security/advisories** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/g/gnutls10/** Currently we are not aware of any exploits for this vulnerability.	GnuTLS Padding Validation Remote Denial of Service CAN-2005-1431	Low	Security Tracker Alert, 1013861, May 2, 2005 Fedora Update Notification, FEDORA-2005-362, May 5, 2005 Gentoo Linux Security Advisory, GLSA 200505-04, May 9, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:084, May 12, 2005** **Ubuntu Security Notice, USN-126-1, May 13, 2005**
GNU Vim 6.x, GVim 6.x	Multiple vulnerabilities exist which can be exploited by local malicious users to gain escalated privileges. The vulnerabilities are caused due to some errors in the modelines options. This can be exploited to execute shell commands when a malicious file is opened. Successful exploitation can lead to escalated privileges but requires that modelines is enabled. Apply patch for vim 6.3: ftp://ftp.vim.org/pub/vim/patches/6.3/6.3.045 Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-10.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-010.html Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-020_RHSA-2005-019.pdf OpenPKG: ftp.openpkg.org Mandrake: http://www.mandrakesecure.net/en/ftp.php Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/v/vim/ SGI: http://support.sgi.com/ Fedora: http://download.fedoralegacy.org/redhat/ **IPCop:** **http://ipcop.org/modules.php?**	GNU Vim / Gvim Modelines Command Execution Vulnerabilities CAN-2004-1138	Medium	Gentoo Linux Security Advisory, GLSA 200412-10 / vim, December 15, 2004 Fedora Legacy Update Advisory, FLSA:2343, February 24, 2005 **Security Focus, 11941, May 11, 2005**

	op=modload&name=Downloads&file=index&req=viewdownload&cid=3&orderby=dateD Currently we are not aware of any exploits for these vulnerabilities.			
GNU zgrep 1.2.4	A vulnerability has been reported in 'zgrep.in' due to insufficient validation of user-supplied arguments, which could let a remote malicious user execute arbitrary commands. A patch for 'zgrep.in' is available in the following bug report: http://bugs.gentoo.org/show_bug.cgi?id=90626 There is no exploit code required.	Gzip Zgrep Arbitrary Command Execution CAN-2005-0758	High	Security Tracker Alert, 1013928, May 10, 2005
HT Editor HT Editor 0.8	Several vulnerabilities have been reported: a vulnerability was reported in the Executable and Linking Format (ELF) parser due to a heap overflow, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability was reported in the Portable Executable (PE) parser due to a boundary error, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200505-08.xml Currently we are not aware of any exploits for these vulnerabilities.	HT Editor ELF & PE Parser Remote Code Execution CAN-2005-1545 CAN-2005-1546	High	Gentoo Linux Security Advisory, GLSA 200505-08, May 10, 2005
KDE KDE 1.1-1.1.2, 1.2, 2.1-2.1.2, 2.2-2.2.2, 3.0-3.0.5, 3.1-3.1.5, 3.2-3.2.3, 3.3-3.3.2	A Denial of Service vulnerability has been reported in the Desktop Communication Protocol (DCOP) daemon due to an error in the authentication process Upgrade available at: http://www.kde.org/download/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-22.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-325.html ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-307.html SUSE: ftp://ftp.SUSE.com/pub/SUSE SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for this vulnerability.	KDE DCOPServer Local Denial of Service CAN-2005-0396	Low	KDE Security Advisory, March 16, 2005 Fedora Update Notifications, FEDORA-2005-244 & 245, March 23, 2005 RedHat Security Advisory, RHSA-2005:325-07, March 23, 2005 ALTLinux Security Advisory, March 29, 2005 RedHat Security Advisory, RHSA-2005:307-08, April 6,2005 SUSE Security Announcement, SUSE-SA:2005:022, April 11, 2005 SGI Security Advisory, 20050403-01-U, April 15, 2005 **Conectiva Linux Security Announcement, CLA-2005:953, May 17, 2005**

KDE kdelibs 3.3.2	A vulnerability exists in the 'dcopidling' library due to insufficient validation of a files existence, which could let a malicious user corrupt arbitrary files. Patch available at: http://bugs.kde.org/attachment.cgi?id=9205&action=view Mandrake: http://www.mandrakesecure.net/en/ftp.php Gentoo: http://security.gentoo.org/glsa/glsa-200503-14.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-325.html ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for this vulnerability.	KDE 'DCOPIDLING' Library CAN-2005-0365	Medium	Security Focus, February 11, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:045, February 18, 2005 Gentoo Linux Security Advisory, GLSA 200503-14, March 7, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:058, March 16, 2005 Fedora Update Notifications, FEDORA-2005-244 & 245, March 23, 2005 RedHat Security Advisory, RHSA-2005:325-07, March 23, 2005 ALTLinux Security Advisory, March 29, 2005 **Conectiva Linux Security Announcement, CLA-2005:953, May 17, 2005**
KDE KDE 3.2-3.2.3, 3.3-3.3.2, 3.4, KDE Quanta 3.1	A vulnerability has been reported due to a design error in Kommander, which could let a remote malicious user execute arbitrary code. Patches available at: ftp://ftp.kde.org/pub/kde/security_patches/f Gentoo: http://security.gentoo.org/glsa/glsa-200504-23.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Ubuntu: http://security.ubuntu.com/Subunit/pool/universe/k/kdewebdev/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for this vulnerability.	KDE Kommander Remote Arbitrary Code Execution CAN-2005-0754	High	KDE Security Advisory, April 20, 2005 Gentoo Linux Security Advisory, GLSA 200504-23, April 22, 200 Fedora Update Notification FEDORA-2005-345, April 28, 2005 Ubuntu Security Notice, USN-115-1, May 03, 2005 **Conectiva Linux Security Announcement, CLA-2005:953, May 17, 2005**
LBL tcpdump 3.4 a6, 3.4, 3.5, alpha, 3.5.2, 3.6.2, 3.6.3, 3.7-3.7.2, 3.8.1 -3.8.3; **IPCop 1.4.1, 1.4.2, 1.4.4, 1.4.5**	Remote Denials of Service vulnerabilities have been reported due to the way tcpdump decodes Border Gateway Protocol (BGP) packets, Label Distribution Protocol (LDP) datagrams, Resource ReSerVation Protocol (RSVP) packets, and Intermediate System to Intermediate System (ISIS) packets. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/t/tcpdump/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-06.xml **Mandriva:** **http://www.mandriva.com/security/advisories** **IPCop:**	LBL TCPDump Remote Denials of Service CAN-2005-1278 CAN-2005-1279 CAN-2005-1280	Low	Bugtraq, 396932, April 26, 2005 Fedora Update Notification, FEDORA-2005-351, May 3, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Ubuntu Security Notice, USN-119-1 May 06, 2005 Gentoo Linux Security Advisory, GLSA 200505-06, May 9, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:087, May 12, 2005**

	http://ipcop.org/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=3&orderby=dateD Exploit scripts have been published.			**Security Focus, 13392, May 12, 2005**
Mozilla Bugzilla 2.17.1, 2.17.3-2.17.7, 2.18 rc1-rc3, 2.19.1, 2.19.2	Several vulnerabilities have been reported: a vulnerability was reported because users can determine if a given invisible product exits when an access denied error is returned, which could let a remote malicious user obtain sensitive information; a vulnerability was reported because bugs can be entered into products that are closed for bug entry when a remote malicious user modifies the URL to specify the name of the product; and a vulnerability was reported because a user's password may be embedded as part of a report URL, which could let a remote malicious user obtain sensitive information. Update available at: http://www.bugzilla.org/download/ There is no exploit code required.	Bugzilla Information Disclosure CAN-2005-1563 CAN-2005-1564 CAN-2005-1565	Medium	Secunia Advisory, SA15338, May 12, 2005
Multiple Vendors Apache Software Foundation Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.6, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.27; Subunit Linux 4.1 pc, ia64, ia32, 5.0 4 power pc, i386, amd64	A buffer overflow vulnerability has been reported in the 'htdigest' utility due to insufficient bounds checking, which could let a remote malicious user potentially execute arbitrary code. Ubuntu: : http://security.ubuntu.com/Subunit/pool/main/a/apache2/ **Proof of Concept exploit scripts have been published.**	Apache 'HTDigest' Buffer Overflow CAN-2005-1344	High	Ubuntu Security Notice, USN-120-1 , May 6, 2005 **Security Focus, 13537, May 14, 2005**
Multiple Vendors KDE 2.0, beta, 2.0.1, 2.1-2.1.2, 2.2-2.2.2, 3.0-3.0.5, 3.1-3.1.5, 3.2-3.2.3, 3.3-3.3.2, 3.4; Novell Linux Desktop 9; SuSE E. Linux 9.1, x86_64, 9.2, x86_64, 9.3, Linux Enterprise Server 9	A buffer overflow vulnerability has been reported in the 'kimgio' image library due to insufficient validation of PCX image data, which could let a remote malicious user cause a Denial of Service or possibly execute arbitrary code. Patches available at: http://bugs.kde.org/attachment.cgi?id=10325&action=view http://bugs.kde.org/attachment.cgi?id=10326&action=view SuSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-22.xml Debian: http://security.debian.org/pool/updates/main/k/kdelibs/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/k/kdelibs/ **Mandriva:** **http://www.mandriva.com/security/advisories** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-393.html** Denial of Service Proofs of Concept exploits have been published.	KDE 'kimgio' image library Remote Buffer Overflow CAN-2005-1046	Low/ High (High if arbitrary code can be executed)	SUSE Security Announcement, SUSE-SA:2005:022, April 11, 2005 Gentoo Linux Security Advisory, GLSA 200504-22, April 22, 2005 Debian Security Advisory, DSA 714-1, April 26, 2005 Fedora Update Notification, FEDORA-2005-350, May 2, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:085, May 12, 2005** **Conectiva Linux Security Announcement, CLA-2005:953, May 17, 2005** **RedHat Security Advisory, RHSA-2005:393-05, May 17, 2005**
Multiple Vendors GNOME GdkPixbuf 0.22 GTK GTK+ 2.4.14	A remote Denial of Service vulnerability has been reported due to a double free error in the BMP loader. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/	GDK-Pixbuf BMP Image Processing Double Free Remote Denial of Service	Low	Fedora Update Notifications, FEDORA-2005-265, 266, 267 & 268, March 30, 2005 RedHat Security

RedHat Fedora Core3 RedHat Fedora Core2	RedHat: http://rhn.redhat.com/errata/RHSA-2005-344.html http://rhn.redhat.com/errata/RHSA-2005-343.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gdk-pixbuf/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SGI: ftp://patches.sgi.com/support/free/security/advisories/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.	CAN-2005-0891		Advisories, RHSA-2005:344-03 & RHSA-2005:343-03, April 1 & 4, 2005 Ubuntu Security Notice, USN-108-1 April 05, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:068 & 069, April 8, 2005 SGI Security Advisory, 20050403-01-U, April 15, 2005 **Turbolinux Security Advisory, TLSA-2005-57, May 16, 2005**
Multiple Vendors Linux kernel 2.2.x, 2.4.x, 2.6.x	A buffer overflow vulnerability has been reported in the 'elf_core_dump()' function due to a signedness error, which could let a malicious user execute arbitrary code with ROOT privileges. Update available at: http://kernel.org/ Trustix: http://www.trustix.org/errata/2005/0022/ An exploit script has been published.	Linux Kernel ELF Core Dump Buffer Overflow CAN-2005-1263	High	Secunia Advisory, SA15341, May 12, 2005 Trustix Secure Linux Security Advisory, 2005-0022, May 13, 2005
Multiple Vendors Linux Kernel 2.6 up to & including 2.6.12-rc4	Several vulnerabilities have been reported: a vulnerability was reported in raw character devices (raw.c) because the wrong function is called before passing an ioctl to the block device, which crosses security boundaries by making kernel address space accessible from user space; and a vulnerability was reported in the 'pkt_ioctl' function in the 'pktcdvd' block device ioctl handler (pktcdvd.c) because the wrong function is called before passing an ioctl to the block device, which could let a malicious user execute arbitrary code. Update available at: http://kernel.org/ A Proof of Concept Denial of Service exploit script has been published.	Multiple Vendor Linux Kernel pktcdvd & raw device Block Device CAN-2005-1264 CAN-2005-1589	High	Secunia Advisory, SA15392, May 17, 2005
Multiple Vendors NASM NASM 0.98.35, 0.98.38; RedHat Advanced Workstation for the Itanium Processor 2.1 IA64, r 2.1, Desktop 3.0, 4.0 RedHat Enterprise Linux WS 4, 3, 2.1 IA64, 2.1, ES 4, 3, 2.1 IA64, 2.1, AS 4, 3, 2.1 IA64, 2.1	A buffer overflow vulnerability has been reported in the 'ieee_putascii()' function, which could let a remote malicious user execute arbitrary code. RedHat: http://rhn.redhat.com/errata/RHSA-2005-381.html **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/n/nasm/** Currently we are not aware of any exploits for this vulnerability.	NASM IEEE_PUTASCII Remote Buffer Overflow CAN-2005-1194	High	RedHat Security Advisory, RHSA-2005:381-06, May 4, 2005 **Ubuntu Security Notice, USN-128-1, May 17, 2005**
Multiple Vendors RedHat Fedora Core3, Core2; Rob Flynn Gaim 1.2; Peachtree Linux release 1	A remote Denial of Service vulnerability has been reported when an unspecified Jabber file transfer request is handled. Upgrade available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo:	Gaim Jabber File Request Remote Denial of Service CAN-2005-0967	Low	Fedora Update Notifications, FEDORA-2005-298 & 299, April 5, 2005 Gentoo Linux Security Advisory, GLSA 200504-05, April 06, 2005 RedHat Security

	http://security.gentoo.org/glsa/glsa-200504-05.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-365.html Mandrake: http://www.mandrakesecure.net/en/ftp.php SGI: http://www.sgi.com/support/security/ Peachtree: http://peachtree.burdell.org/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/g/gaim/** **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** There is no exploit code required.			Advisory, RHSA-2005:365-06, April 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:071, April 14, 2005 SGI Security Advisory, 20050404-01-U, April 20, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 Conectiva Linux Security Announcement, CLA-2005:949, April 27, 2005 **Ubuntu Security Notice, USN-125-1, May 12, 2005** **Slackware Security Advisory, SSA:2005-133-01, May 13, 2005**
Multiple Vendors RedHat Fedora Core3, Core2; Rob Flynn Gaim 1.2; Ubuntu Linux 4.1 ppc, ia64, ia32; Peachtree Linux release 1	Two vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported due to a buffer overflow in the 'gaim_markup_strip_html()' function; and a vulnerability has been reported in the IRC protocol plug-in due to insufficient sanitization of the 'irc_msg' data, which could let a remote malicious user execute arbitrary code. Update available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-05.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-365.html Mandrake: http://www.mandrakesecure.net/en/ftp.php SGI: http://www.sgi.com/support/security/ Peachtree: http://peachtree.burdell.org/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** Currently we are not aware of any exploits for these vulnerabilities.	Gaim 'Gaim_Markup_Strip_HTML()' Function Remote Denial of Service & IRC Protocol Plug-in Arbitrary Code Execution CAN-2005-0965 CAN-2005-0966	Low/ High (High if arbitrary code can be executed)	Fedora Update Notifications, FEDORA-2005 -298 & 299, April 5, 2005 Ubuntu Security Notice, USN-106-1 April 05, 2005 Gentoo Linux Security Advisory, GLSA 200504-05, April 06, 2005 RedHat Security Advisory, RHSA-2005:365-06, April 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:071, April 14, 2005 SGI Security Advisory, 20050404-01-U, April 20, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 Conectiva Linux Security Announcement, CLA-2005:949, April 27, 2005 **Slackware Security Advisory, SSA:2005-133-01, May 13, 2005**

Multiple Vendors X.org X11R6 6.7.0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1.0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3.0.2, 4.3.0.1, 4.3.0	An integer overflow vulnerability exists in 'scan.c' due to insufficient sanity checks on on the 'bitmap_unit' value, which could let a remote malicious user execute arbitrary code. Patch available at: https://bugs.freedesktop.org/attachment.cgi?id=1909 Gentoo: http://security.gentoo.org/glsa/glsa-200503-08.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lesstif1-1/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xfree86/ ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-331.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-044.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/x/xfree86/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-412.html** Currently we are not aware of any exploits for this vulnerability.	LibXPM Bitmap_unit Integer Overflow CAN-2005-0605	High	Security Focus, 12714, March 2, 2005 Gentoo Linux Security Advisory, GLSA 200503-08, March 4, 2005 Ubuntu Security Notice, USN-92-1 March 07, 2005 Gentoo Linux Security Advisory, GLSA 200503-15, March 12, 2005 Ubuntu Security Notice, USN-97-1 March 16, 2005 ALTLinux Security Advisory, March 29, 2005 Fedora Update Notifications, FEDORA-2005 -272 & 273, March 29, 2005 RedHat Security Advisory, RHSA-2005: 331-06, March 30, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 RedHat Security Advisory, RHSA-2005:044-15, April 6, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:080, April 29, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:081, May 6, 2005 Debian Security Advisory, DSA 723-1, May 9, 2005 **RedHat Security Advisory, RHSA-2005:412-05, May 11, 2005**
PixySoft Guestbook Pro 3.2.1 & prior	A Cross-Site Scripting vulnerability has been reported due to insufficient validation of user-supplied input in the message content and title fields, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	PixySoft Guestbook Pro Cross-Site Scripting CAN-2005-1557	High	Security Tracker Alert, 1013940, May 11, 2005
PostgreSQL PostgreSQL 7.3 through 8.0.2	Two vulnerabilities have been reported: a vulnerability was reported because a remote authenticated malicious user can invoke some client-to-server character set conversion functions and supply specially crafted argument values to potentially execute arbitrary commands; and a remote Denial of Service vulnerability was reported because the 'contrib/tsearch2' module incorrectly declares several functions as returning type 'internal.' Fix available at: http://www.postgresql.org/about/news.315 Trustix: http://http.trustix.org/pub/trustix/updates/	PostgreSQL Remote Denial of Service & Arbitrary Code Execution CAN-2005-1409 CAN-2005-1410	Low/ High (High if arbitrary code can be executed)	Security Tracker Alert, 1013868, May 3, 2005 Ubuntu Security Notice, USN-118-1, May 04, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 **Gentoo Linux Security Advisory, GLSA 200505-12, May 16,**

	Gentoo: **http://security.gentoo.org/glsa/glsa-200505-12.xml** **Trustix:** **http://www.trustix.org/errata/2005/0023/** Currently we are not aware of any exploits for these vulnerabilities.			**2005** **Trustix Secure Linux Bugfix Advisory, TSL-2005-0023, May 16, 2005**
Pserv Pserv 3.2	A buffer overflow vulnerability has been reported in 'completedPath' due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://prdownloads.sourceforge.net/pserv/pserv-3.3.tar.gz?download Currently we are not aware of any exploits for this vulnerability.	Pserv 'completedPath' Remote Buffer Overflow CAN-2005-1626	High	Security Focus, 13648, May 16, 2005
Pserv Pserv 3.2	Several vulnerabilities have been reported: a Directory Traversal vulnerability was reported due to insufficient filtering of URIs, which could let a remote malicious user obtain sensitive information; a vulnerability has been reported when a specially crafted URI request is handled, which could let a remote malicious user obtain sensitive information; and a vulnerability was reported because the web server does not differentiate between files and symbolic links, which could let a malicious user obtain sensitive information. Upgrade available at: http://prdownloads.sourceforge.net/pserv/pserv-3.3.tar.gz?download There is no exploit code required; however, Proofs of Concept exploits have been published.	PServ Remote Directory Traversal & Information Disclosure CAN-2005-1365 CAN-2005-1366 CAN-2005-1367	Medium	Security Focus, 13638 & 13642, May 16, 2005
SCO Unixware 7.1.1, 7.1.3, 7.1.4	A vulnerability exists in the 'chroot()' feature due to errors in the implementation, which could let a malicious user break out of the chroot restriction and access arbitrary files. Patches available at: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.2 **ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.22** An exploit script has been published.	SCO UnixWare 'CHRoot()' Feature Breakout CVE Name: CAN-2004-1124	Medium	SCO Security Advisory, SCOSA-2005.2, January 14, 2005 **SCO Security Advisory, SCOSA-2005.22, May 11, 2005**
Sun Microsystems, Inc. Solaris 7.0, _x86, 8.0, _x86, 9.0, _x86	A Denial of Service vulnerability has been reported in the automountd daemon. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57786-1 Currently we are not aware of any exploits for this vulnerability.	Sun Solaris automountd Denial of Service CAN-2005-1518	Low	Sun(sm) Alert Notification, 57786, May 10, 2005
SWSoft Confixx Pro 3, Confixx 3.0.6, 3.0.8	An SQL injection vulnerability has been reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. **Hotfix available at:** **http://download1.sw-soft.com/Confixx/Confixx Pro3/3.0.8/confixx_v3.0.8-build20050505.10_php_hotfix.sh.gz** There is no exploit code required.	SWSoft Confixx SQL Injection CAN-2005-1302	High	Security Focus, 13355, April 25, 2005 **Security Focus, 13366, May 16, 2005**
Viewglob Viewglob 2.x	A vulnerability has been reported in the 'vgs' server program when handling 'vgseer' clients, which could let a malicious user obtain sensitive information. Update available at: http://viewglob.sourceforge.net/download.html Currently we are not aware of any exploits for this vulnerability.	Viewglob Information Disclosure CAN-2005-1627	Medium	Security Tracker Alert, 1013937, May 11, 2005
WebAPP WebAPP 0.9.9.2.1, 0.9.9.2, 0.9.9	A vulnerability has been reported in 'apage.cgi' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary commands. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	WebAPP 'apage.cgi' Remote Command Execution CAN-2005-1628	High	Security Focus, 13637, May 16, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
1two.org 1Two News 1.0	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the 'index.php' script due to insufficient validation of several parameters, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported in the 'delete.php' script because images associated with news postings can be removed; and a vulnerability was reported in the 'admin/upload.php' script because a remote malicious user can upload images. No workaround or patch available at time of publishing. There is no exploit code required.	1Two News Cross-Site Scripting & Image Deletion & Upload CAN-2005-1582 CAN-2005-1583	High	SecurityTracker Alert, 1013960, May 12, 2005
Acrowave AAP-3100AR Route	A vulnerability has been reported due to an error in the authentication process, which could let a remote malicious user bypass security restrictions and obtain administrative access. No workaround or patch available at time of publishing. There is no exploit code required.	Acrowave AAP-3100AR Wireless Router Authentication Bypass CAN-2005-1566	High	Bugtraq, 398060, May 12, 2005
All Enthusiast Inc. Photopost PHP Pro 3.1-3.3, 4.0, 4.1, 4.6, 4.8.1, 5.0 RC3	An SQL injection vulnerability was reported in the 'member.php' script due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	All Enthusiast PhotoPost PHP Pro 'Member.PHP' SQL Injection CAN-2005-1629	High	Security Focus, 13620, May 13, 2005
Attachment Mod Attachment Mod 2.3.11, 2.3.12	A vulnerability has been reported when handling realnames due to an unspecified error. The impact was not specified. Upgrades available at: http://prdownloads.sourceforge.net/acydmods/attach_mod_2313-files.tar.gz?download Currently we are not aware of any exploits for this vulnerability.	Attachment Mod Unspecified Realname CAN-2005-1630	Not Specified	Secunia Advisory, SA15327, May 13, 2005
BoastMachine BoastMachine 3.0 platinum	An input validation vulnerability has been reported in 'users.ini.php,' which could let a remote malicious user upload arbitrary files and execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	BoastMachine File Upload CAN-2005-1580	High	Security Focus, 13600, May 11, 2005
Booby Booby 1.0 .0 & prior	A vulnerability has been reported in 'booby.php' due to an error, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://prdownloads.sourceforge.net/booby/booby-1.0.1-2_May_2005.tar.gz?download There is no exploit code required.	Booby Private Bookmark Disclosure CAN-2005-1631	Medium	Secunia Advisory, SA15305, May 13, 2005
Cisco Systems FWSM for Cisco Catalyst 6500/7600 Series, 6500/7600 Series 1.1 (3.17), 6500/7600 Series 2.3.1	A vulnerability has been reported when enforcing URL, FTP, or HTTPS filtering, which could let a remote malicious user bypass access control lists (ACLs). Upgrade and workaround information available at: http://www.cisco.com/warp/public/707/cisco-sa-20050511-url.shtml There is no exploit code required.	Cisco FWSM URL, FTP, & HTTPS Filtering ACL Bypass CAN-2005-1517	Medium	Cisco Security Advisory, 64821, May 11, 2005
DirectTopics.nl DirectTopics DT 2final, 2beta, DirectTopics 2.1, 2.2	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'topic.php' due to insufficient sanitization of the 'topic' parameter, which could let a remote malicious user execute arbitrary SQL code and obtain sensitive information; and a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of certain passed in BB code, which could let ak remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Direct Topics SQL Injection & Cross-Site Scripting CAN-2005-1567 CAN-2005-1568 CAN-2005-1569	High	Secunia Advisory, SA15353, May 13, 2005

Eric Fichot Bug Report 1.0	A Cross-Site Scripting vulnerability has been reported in the 'bug_report.php' script due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Eric Fichot Bug Report 'bug_report.php' Cross-Site Scripting CAN-2005-1581	High	Security Tracker Alert, 1013957, May 12, 2005
Iansoft Enterprises OpenBB 1.0.8	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in the 'Read.php' script due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in the 'Member.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	OpenBB SQL Injection & Cross-Site Scripting CAN-2005-1612 CAN-2005-1613	High	Bugtraq, 398162, May 13, 2005
JGS-XA Support JGS-Portal 3.0.1, 3.0.2	Multiple Cross-Site Scripting and SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code and HTML and script code. It is also possible to obtain the full path to certain scripts by accessing them directly. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	JGS-Portal Multiple Cross-Site Scripting & SQL Injection CAN-2005-1633 CAN-2005-1634 CAN-2005-1635	High	Bugtraq, 398315, May 16, 2005
Macromedia, Inc. ColdFusion MX 7.0	A Cross-Site Scripting vulnerability has been reported in the default error page due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Patch available at: http://download.macromedia.com/pub/coldfusion/hotfix/chf70-60112.jar There is no exploit code required.	Macromedia ColdFusion MX 7 Default Error Page Cross-Site Scripting CAN-2005-1555	High	Macromedia Security Bulletin, MPSB05-03, May 10, 2005
Mozilla.org Mozilla Browser 1.0-1.0.2, 1.1-1.7.6, Firefox 0.8-0.10.1, 1.0.1, 1.0.2; Netscape Navigator 7.0, 7.0.2, 7.1, 7.2, 7.0-7.2	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'EMBED' tag for non-installed plugins when processing the 'PLUGINSPAGE' attribute due to an input validation error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because blocked popups that are opened through the GUI incorrectly run with 'chrome' privileges, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the global scope of a window or tab are not cleaned properly before navigating to a new web site, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the URL of a 'favicons' icon for a web site isn't verified before changed via JavaScript, which could let a remote malicious user execute arbitrary code with elevated privileges; a vulnerability was reported because the search plugin action URL is not properly verified before used to perform a search, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to the way links are opened in a sidebar when using the '_search' target, which could let a remote malicious user execute arbitrary code; several input validation vulnerabilities were reported when handling invalid type parameters passed to 'InstallTrigger' and 'XPInstall' related objects, which could let a remote malicious user execute arbitrary code; and vulnerabilities were reported due to insufficient validation of DOM nodes in certain privileged UI code, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.mozilla.org/products/firefox/ http://www.mozilla.org/products/mozilla1.x/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-18.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-383.html http://rhn.redhat.com/errata/RHSA-2005-386.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/	Mozilla Suite / Firefox Multiple Vulnerabilities CAN-2005-0752 CAN-2005-1153 CAN-2005-1154 CAN-2005-1155 CAN-2005-1156 CAN-2005-1157 CAN-2005-1158 CAN-2005-1159 CAN-2005-1160	High	Mozilla Foundation Security Advisories, 2005-35 - 2005-41, April 16, 2005 Gentoo Linux Security Advisory, GLSA 200504-18, April 19, 2005 US-CERT VU#973309 RedHat Security Advisories, RHSA-2005:383-07 & RHSA-2005-386., April 21 & 26, 2005 Turbolinux Security Advisory, TLSA-2005-49, April 21, 2005 US-CERT VU#519317 SUSE Security Announcement, SUSE-SA:2005:028, April 27, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 **Ubuntu Security Notice, USN-124-1 & USN-124-2, May 11 & 12, 2005** **Mandriva Linux Security Update Advisory,**

	errata/RHSA-2005-384.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/** **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.			**MDKSA-2005:088, May 14, 2005**
Mozilla.org Mozilla Suite prior to 1.7.6, Firefox prior to 1.0.2	A vulnerability has been reported when processing drag and drop operations due to insecure XUL script loading, which could let a remote malicious user execute arbitrary code. Mozilla Browser: http://www.mozilla.org/products/mozilla1.x/ Firefox: http://www.mozilla.org/products/firefox/ Fedora: http://download.fedora.red hat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml http://security.gentoo.org/glsa/glsa-200503-31.xml Slackware: http://slackware.com/security/viewer.php?El=slackware-security&ay=2005&m=slackware-security.000123 RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Mandriva:** **http://www.mandriva.com/security/advisories** A Proof of Concept exploit has been published.	Mozilla Suite/ Firefox Drag and Drop Arbitrary Code Execution CAN-2005-0401	High	Mozilla Foundation Security Advisory 2005-32, March 23, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 SGI Security Advisory, 20050501 -01-U, May 5, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:088, May 14, 2005**
Mozilla Firefox 1.0	A vulnerability exists in the XPCOM implementation that could let a remote malicious user execute arbitrary code. The exploit can be automated in conjunction with other reported vulnerabilities so no user interaction is required. A fixed version (1.0.1) is available at: http://www.mozilla.org/products/firefox/all.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Mandriva:** **http://www.mandriva.com/security/advisories** A Proof of Concept exploit has been published.	Mozilla Firefox Remote Code Execution Vulnerability CAN-2005-0527	High	Security Tracker Alert ID: 1013301, February 25, 2005 Gentoo Linux Security Advisory GLSA 200503-30. March 25, 2005 SGI Security Advisory, 20050501 -01-U, May 5, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:088, May 14, 2005**

Mozilla Firefox Preview Release, 0.8, 0.9 rc, 0.9-0.9.3, 0.10, 0.10.1, 1.0-1.0.3	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient protection of 'IFRAME' JavaScript URLS from being executed in the context of another history list URL, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'InstallTrigger .install()' due to insufficient verification of the 'Icon URL' parameter, which could let a remote malicious user execute arbitrary JavaScript code. Workaround: Disable "tools/options/web-Features/>Allow web sites to install software" **Slackware:** **ftp://ftp.slackware.com/pub/slac ware/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-11.xml** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Proofs of Concept exploit scripts have been published.	Mozilla Firefox Remote Arbitrary Code Execution CAN-2005-1476 CAN-2005-1477	High	Secunia Advisory, SA15292, May 9, 2005 US-CERT VU#534710 US-CERT VU#648758 **Slackware Security Advisory, SSA:2005-135-01, May 15, 2005** **Gentoo Linux Security Advisory, GLSA 200505-11, May 16, 2005** **Turbolinux Security Advisory, TLSA-2005-56, May 16, 2005**
Mozilla Mozilla 0.x, 1.0, 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7.x Mozilla Firefox 0.x Mozilla Thunderbird 0.x	Multiple vulnerabilities exist in Firefox, Mozilla and Thunderbird that can permit users to bypass certain security restrictions, conduct spoofing and script insertion attacks and disclose sensitive and system information. Mozilla: Update to version 1.7.5: http://www.mozilla.org/products/mozilla1.x/ Firefox: Update to version 1.0: http://www.mozilla.org/products/firefox/ Thunderbird: Update to version 1.0: http://www.mozilla.org/products/thunderbird/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?El=slackware-security&y=2005&m=slackware-security.000123 RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for these vulnerabilities.	Mozilla Firefox, Mozilla, and Thunderbird Multiple Vulnerabilities CAN-2005-0141 CAN-2005-0143 CAN-2005-0144 CAN-2005-0145 CAN-2005-0146 CAN-2005-0147 CAN-2005-0148 CAN-2005-0149 CAN-2005-0150	Medium/ High (High if arbitrary code can be executed)	Mozilla Foundation Security Advisory 2005-01, 03, 04, 07, 08, 09, 10, 11, 12 Fedora Update Notification, FEDORA-2005-248, 249, 251, 253, March 23 & 25, 2005 Slackware Security Advisory, SSA:2005-085-01, March 27, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:088, May 14, 2005**
Mozilla Mozilla Browser prior to 1.7.8; Mozilla Suite prior to 1.7.8; Firefox prior to 1.0.4; Firebird 0.5, 0.6.1, 0.7	A vulnerability was reported due to a failure in the application to properly verify Document Object Model (DOM) property values, which could let a remote malicious user execute arbitrary code. Firefox: http://www.mozilla.org/products/firefox/ Mozilla Browser Suite: http://www.mozilla.org/products/mozilla1.x/ TurboLinux:: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Currently we are not aware of any exploits for this vulnerability.	Mozilla Suite And Firefox DOM Property Overrides CAN-2005-1532	High	Mozilla Foundation Security Advisory, 2005-44, May 12, 2005 Turbolinux Security Advisory, TLSA-2005-56, May 16, 2005
Mozilla Mozilla Browser prior to 1.7.8; Mozilla Suite prior to 1.7.8; Firefox prior to	A vulnerability was reported when processing 'javascript:' URLs, which could let a remote malicious user execute arbitrary code. Firefox: http://www.mozilla.org/	Mozilla Suite And Firefox Wrapped 'javascript:' URLs	High	Mozilla Foundation Security Advisory, 2005-43, May 12, 2005

1.0.4; Firebird 0.5, 0.6.1, 0.7	products/firefox/ Mozilla Browser Suite: http://www.mozilla.org/products/mozilla1.x/ TurboLinux:: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Currently we are not aware of any exploits for this vulnerability.	CAN-2005-1531		Turbolinux Security Advisory, TLSA-2005-56, May 16, 2005
Multiple Vendors Squid Web Proxy Cache2.5.STABLE9 & prior	A vulnerability has been reported in the DNS client when handling DNS responses, which could let a remote malicious user spoof DNS lookups. Patch available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE9-dns_query-4.patch Trustix: http://www.trustix.org/errata/2005/0022/ Currently we are not aware of any exploits for this vulnerability.	Squid Proxy DNS Spoofing CAN-2005-1519	Medium	Security Focus, 13592, May 11, 2005 Trustix Secure Linux Security Advisory, 2005-0022, May 13, 2005
Multiple Vendors IETF RFC 2406: IPSEC; **Hitachi GR2000-1B, GR2000-2B, GR2000-2B+, GR2000-BH**	A vulnerability has been reported that affects certain configurations of IPSec when configured to employ Encapsulating Security Payload (ESP) in tunnel mode with only confidentiality and systems that use Authentication Header (AH) for integrity protection, which could let a remote malicious user obtain plaintext IP datagrams and potentially sensitive information. **Hitachi advises affected users to use the AH protocol workaround to mitigate this issue.** Currently we are not aware of any exploits for this vulnerability.	IPSec ESP Packet Modification CAN-2005-0039	Medium	NISCC Vulnerability Advisory, IPSEC - 004033, May 9, 2005 **US-CERT VU#302220** **Security Focus, 13562, May 11, 2005**
Multiple Vendors MandrakeSoft Linux Mandrake 10.2 X86_64, 10.2; Rob Flynn Gaim 0.10 x, 0.10.3, 0.50-0.75, 0.78, 0.82, 0.82.1, 1.0-1.0.2, 1.1.1-1.1.4, 1.2, 1.2.1; Ubuntu Linux 4.1 ppc, ia64, ia32, 5.0 4 powerpc, i386, amd64	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported when handling long URIs due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability was reported due to a NULL pointer dereference error when handling MSN messages. Rob Flynn: http://prdownloads.sourceforge.net/gaim/gaim-1.3.0.tar.gz?download RedHat: http://rhn.redhat.com/errata/RHSA-2005-429.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-09.xml Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ A Proof of Concept exploit script has been published.	Gaim Remote Buffer Overflow & Denial of Service CAN-2005-1261 CAN-2005-1262	Low/ High (High if arbitrary code can be executed)	Fedora Update Notification, FEDORA-2005-369, May 11, 2005 RedHat Security Advisory, RHSA-2005:429-06, May 11, 2005 Gentoo Linux Security Advisory, GLSA 200505-09, May 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:086, May 12, 2005 Ubuntu Security Notice, USN-125-1, May 12, 2005
MySQL AB MySQL 4.0 .0-4.0.11, 5.0 .0- 5.0.4	A vulnerability has been reported in the 'mysql_install_db' script due to the insecure creation of temporary files, which could let a malicious user obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required.	MySQL 'mysql_install_db' Insecure Temporary File Creation CAN-2005-1636	Medium	Security Focus, 13660, May 17, 2005
Neteyes NexusWay	Multiple vulnerabilities have been reported: a vulnerability was reported in the web module due to weak authentication, which could let a remote malicious user change device configuration; a vulnerability was reported because a remote malicious user can access Shell or execute any command with ROOT privileges when a specially crafted argument is submitted in a certain command; and a vulnerability was reported when a remote malicious user submits specially crafted packets to a certain administrative script, which could lead to the execution of arbitrary code with ROOT privileges. No workaround or patch available at time of publishing.	Neteyes NexusWay Border Gateway Multiple Remote Vulnerabilities CAN-2005-1558 CAN-2005-1559 CAN-2005-1560	High	Scan Associates Advisory, May 11, 2005

	There is no exploit code required; however, Proofs of Concept exploits have been published.			
NPDS NPDS 4.8, 5.0	SQL injections vulnerabilities have been reported in the 'comments.php' and 'pollcomments.php' scripts due to insufficient validation of the 'thold' parameter, which could let a remote malicious user execute arbitrary SQL code. Update available at: http://www.npds.org/ article.php?sid=1254&thold=0 There is no exploit code required; however, Proofs of Concept exploits have been published.	NPDS Input Validation CAN-2005-1637	High	Security Tracker Alert, 1013973, May 16, 2005
Open Solution Quick.Cart 0.3	Several vulnerabilities were reported: a Cross-Site Scripting vulnerability was reported in 'index.php' due to insufficient sanitization of the 'sWord' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in 'index.php' due to insufficient sanitization of the 'iCategory' parameter before used in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Open Solution Quick.Cart Cross-Site Scripting & SQL Injection CAN-2005-1587 CAN-2005-1588	High	Lostmon´s Blogger, May 11, 2005
Open Solution Quick.Forum 2.1.6	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'index.php' due to insufficient sanitization of the 'topic' field, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in 'index.php' due to insufficient sanitization of input passed to the 'iCategory' and 'page' variables, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	Open Solution Quick.Forum Cross-Site Scripting & SQL Injection CAN-2005-1584 CAN-2005-1585 CAN-2005-1586	High	Lostmon´s Blogger, May 11, 2005
phpBB Group phpBB prior to 2.0.15	A vulnerability has been reported in 'includes/bbcode.php' due to insufficient validation of the user-supplied BBCode URLs in the 'make_clickable()' function, which could let a remote malicious user execute arbitrary code. Update available at: http://www.phpbb.com/ downloads.php **A Proof of Concept exploit has been published.**	phpBB 'bbcode.php' Input Validation CAN-2005-1193	High	Security Tracker Alert, 1013918, May 9, 2005 **US-CERT VU#113196**
phpHeaven phpMyChat 0.14.5	A Cross-Site Scripting vulnerability has been reported in the 'Start-Page.CSS.php3' and 'Style.CSS.php3' scripts due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPHeaven PHPMyChat Cross-Site Scripting CAN-2005-1619	High	Bugtraq, 398167, May 14, 2005
PostNuke Development Team PostNuke 0.75, 0.76 RC4	A Directory Traversal vulnerability has been reported in the 'Blocks' module when a name is submitted for a target file, which could let a remote malicious user obtain sensitive information. Patches available at: http://cvs.postnuke.com/ viewcvs.cgi/Historic_ PostNuke_Library/ postnuke-devel/html/ There is no exploit code required; however, a Proof of Concept exploit has been published.	PostNuke Blocks Module Directory Traversal CAN-2005-1621	Medium	Security Focus, 13636, May 16, 2005
Roman Ivanov SafeHTML 1.1-1.3.1	A vulnerability has been reported due to an error in the quotes handling of attributes values in '_writeAttrs(),' which could let a remote malicious user execute arbitrary HTML code. Upgrades available at: http://pixel-apes.com/ download/safehtml-1.3.2.zip There is no exploit code required.	SafeHTML Quotes Handling Arbitrary HTML Execution CAN-2005-1638	High	Secunia Advisory, SA15371, May 17, 2005
Skull-Splitter Guestbook 1.0, 2.0, 2.2	Multiple vulnerabilities have been reported in the title and content of posted messages because it is possible to inject arbitrary HTML and code, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Skull-Splitter Guestbook Multiple HTML Injection CAN-2005-1620	High	Security Focus,13632, May 14, 2005
Sun Microsystems, Inc. StorEdge 6130 Array	A vulnerability has been reported in Sun StorEdge 6130 controller arrays with a serial number in the range of 0451AWF00G - 0513AWF00J, which could let a local/remote malicious user obtain unauthorized access.	Sun StorEdge 6130 Array Unauthorized Access	Medium	Sun(sm) Alert Notification, 57771, May 5, 2005

	Sun recommends that customers contact their Sun authorized service provider to obtain fixes. There is no exploit code required.	CAN-2005-1609		US-CERT VU#812438
The Ignition Project ignitionServer 0.3 .0, 0.3.1, -P1, beta1, 0.3.2 beta2, 0.3.3 beta3, 0.3.4 a beta4, 0.3.6	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient access validation before allowing a host to delete entries, which breaches channel security and allows hosts to delete access entries set by owners; and a vulnerability was reported because IRC operators can't access channels created and locked by normal users due to a design error. Patches available at: http://www.ignition-project.com/download/ There is no exploit code required.	ignitionServer Access Entry Deletion & Channel Locking CAN-2005-1640 CAN-2005-1641	Medium	The Ignition Project Security Bulletin, May 15, 2005
Tim Hoeppner Ultimate PHP Board 1.8, 1.8.2, 1.9, 1.9.6	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the 'ViewForum.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in the 'ViewForum.php' script due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Ultimate PHP Board Cross-Site Scripting & SQL Injection CAN-2005-1614 CAN-2005-1615	High	Security Focus, 13621 & 13622, May 13, 2005
Woltlab Burning Board 2.0 RC1 & RC2, beta 3-beta 5, 2.3.1	An SQL injection vulnerability has been reported in the 'verify_email()' function due to insufficient sanitization of input passed to the 'email' field when registering or updating an account, which could let a remote malicious user execute arbitrary SQL code. Contact the vendor for a patch. There is no exploit code required.	WoltLab Burning Board 'Verify_email' Function SQL Injection CAN-2005-1642	High	GulfTech Security Research Advisory, May 16, 2005
WordPress WordPress 1.5	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'WP-Trackback.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in 'Post.PHP' and 'Edit.PHP' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://wordpress.org/latest.tar.gz There is no exploit code required; however, a Proof of Concept exploit has been published.	Wordpress SQL Injection & Cross-Site Scripting	High	Security Focus, 13655, 13663, & 13664, May 17, 2005
Zoidcom Zoidcom 1.0 beta 4 & prior	A remote Denial of Service vulnerability has been reported in the 'ZCom_BitStream::Deserialize' function. Update available at: http://www.zoidcom.com/download.html A Proof of Concept exploit has been published.	Zoidcom 'ZCom_BitStream::Deserialize()' Function Remote Denial of Service CAN-2005-1643	Low	Security Tracker Alert, 1013939, May 11, 2005

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
May 17, 2005	LandIpV6.cpp	No	Script that exploits the Microsoft IPV6 TCPIP Loopback LAND Denial of Service vulnerability.
May 17, 2005	pktcdvd_dos.c	No	Proof of Concept Denial of Service exploit for the Multiple Linux Kernel IOCTL Handlers Local Memory Corruption vulnerability.
May 16, 2005	htdigest-realm-bof.c htexploit.c	Yes	Proofs of Concept exploit scripts for the Apache 'HTDigest' Buffer Overflow vulnerability.
May 14, 2005	vuln-plugin.so	Yes	Proof of Concept exploit for the Gaim Remote Buffer Overflow & Denial of Service vulnerability.
May 13, 2005	netvault_hof.c	No	Script that exploits the BakBone NetVault Remote Heap Overflow Code Execution vulnerability.

May 13, 2005	photopost_sql	No	Proof of Concept exploit script for the All Enthusiast PhotoPost PHP Pro 'Member.PHP' SQL Injection vulnerability.
May 11, 2005	ethereal_sip_dos.c	Yes	Script that exploits the Ethereal Multiple Remote Protocol Dissector Vulnerabilities.
May 10, 2005	elfcd.sh	Yes	Script that exploits the Linux Kernel ELF Core Dump Buffer Overflow vulnerability.

[back to top]

Trends

- **Phishing gets personal:** According to the anti-fraud software firm, Cyota, fraudsters are using stolen information to lure victims into divulging additional sensitive information in a new form of phishing attack. Crooks are using real information about the accountholder. Personalized phishing attacks seek to supplement existing lists of stolen credentials with even more sensitive information, such as ATM PIN numbers or credit card CVV codes. Source: http://www.theregister.co.uk/2005/05/17/personal_phishing/.
- **MasterCard and Cyota: Anti-phishing trends:** On Tuesday, May 10th, MasterCard International Inc. said that it had shut down nearly 1,400 phishing sites and more than 750 sites suspected of selling illegal credit-card information since launching an ID-theft-prevention program in June. The program also has led to the discovery and protection of more than 35,000 MasterCard account numbers that were in jeopardy of being compromised. Source: http://www.crime-research.org/news/12.05.2005/1228/.
- **Symbian success feeds mobile malware explosion**: Mobile phone malware is still at an embryonic stage when compared with viruses and Trojan horses that target the Windows operating system. However, experts say this is because there is currently such a diverse range of mobile phone operating systems. However, if over the next few years Symbian manages to grab a large enough share of the mobile OS market, it could create a new front in the war against malicious software. Source: http://www.zdnet.com.au/news/security/0,2000061744,39191477,00.htm.
- **Extortion via DDoS on the rise:** Criminals are increasingly targeting corporations with Distributed Denial of Service (DDoS) attacks designed not to disrupt business networks but to be used as tools to extort thousands of dollars from the companies. Experts claim that those targeted are increasingly deciding to pay the extortionists rather than accept the consequences. Source: http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,101761,00.html?SKC=cybercrime-101761.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Netsky-Q	Win32 Worm	Increase	March 2004
3	Mytob.C	Win32 Worm	Slight Decrease	March 2004
4	Zafi-D	Win32 Worm	Slight Decrease	December 2004
5	Netsky-D	Win32 Worm	Increase	March 2004
6	Lovgate.w	Win32 Worm	Increase	April 2004
7	Zafi-B	Win32 Worm	Decrease	June 2004
7	Netsky-Z	Win32 Worm	Increase	April 2004
9	Netsky-B	Win32 Worm	Decrease	February 2004
10	MyDoom-O	Win32 Worm	New to Table	July 2004

Table Updated May 17, 2005

Viruses or Trojans Considered to be a High Level of Threat

- **Sober.q**: Sober.q uses both German and English-language messages to direct recipients to Web sites with right-wing German nationalistic content, according to an advisory from e-mail security company MX Logic. One of the URLs points to the Web site of the right-wing German NPD party, it says. The variant is downloaded by computers already infected by the Sober.p worm, which began circulating earlier this month. Source: http://www.pcworld.com/resource/article/0,aid,120846,pg,1,RSS,RSS,00.asp

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Sdbot.AQ		Trojan

Downloader-AAP		Trojan
Kelvir.AS	Trj/Kelvir.AS	Trojan
Sdbot.DKE	W32/Sdbot.DKE.worm	Win32 Worm
Sircam	I-Worm.Sircam W32.Sircam W32/SircCam	Win32 Worm
Sober.Q	Email-Worm.Win32.Sober.q Troj/Sober-Q W32/Sober.q@MM WORM_SOBER.U	Win32 Worm
Totilix	I-Worm.Totilix	Win32 Worm
Troj/Banker-HC		Trojan
Troj/Goldun-T	Trojan-Dropper.Win32.Agent.ku Trojan-Spy.Win32.Goldun.ar Trojan-Spy.Win32.Goldun.aq	Trojan
Troj/Haxdoor-Y		Trojan
Troj/Saye-A	Exploit-DcomRpc.gen Hacktool.DCOMScan Net-Worm.Win32.Padobot.z W32.Ifbo.A	Trojan
Troj/Sqdrop-A		Trojan
Trojan.Ascetic.C	W32.Sober.P@mm	Win32 Worm
Trojan.Esteems.C		Trojan
Trojan.Esteems.D		Win32 Worm
Trojan.Flush.D		Trojan
Trojan.Jasbom		Trojan
Trojan.Lukuspam		Trojan
Trojan.Olfeb.A		Trojan
Trojan.Pepop		Trojan
VBS.Soraci.B		Visual Basic Worm
W32.Alcan.A	W32.Alcra.A	Win32 Worm
W32.Lanieca.A@mm		Win32 Worm
W32.Mydoom.BT@mm		Win32 Worm
W32.Mytob.CE@mm		Win32 Worm
W32.Mytob.CF@mm		Win32 Worm
W32.Mytob.CH@mm		Win32 Worm
W32.Randex.DXP		Win32 Worm
W32.Yaha.H@mm	I-Worm.Lentin.H Lentin.H W32/Lentin.G@mm Yaha.H Yaha.J	Win32 Worm
W32/Agobot-SE	Backdoor.Win32.Agobot.ace	Win32 Worm
W32/Agobot-SF	Backdoor.Win32.Agobot.acb WORM_GAOBOT.CW	Win32 Worm
W32/Agobot-SJ	W32/Sdbot.worm.gen.j WORM_AGOBOT.AUC	Win32 Worm
W32/Eyeveg-F	Worm.Win32.Eyeveg.f W32/Eyeveg.worm.gen	Win32 Worm
W32/Eyeveg-G	Worm.Win32.Eyeveg.f W32/Eyeveg.worm.gen WORM_WURMARK.J	Win32 Worm
W32/Kelvir-Gen		Win32 Worm
W32/Korvar	Braid.C HLLM.Seoul I-Worm.Winevar Korvar W32.HLLW.Winevar Win32.HLLM.Seoul Winevar WORM_WINEVAR.A	Win32 Worm
W32/Mytob-AZ	Net-Worm.Win32.Mytob.au	Win32 Worm
W32/Mytob-CA		Win32 Worm
W32/Mytob-CH	WORM_MYTOB.DA	Win32 Worm
W32/Mytob-CI	Email-Worm.Win32.Mydoom.am	Win32 Worm
W32/Mytob-CJ		Win32 Worm
W32/Oscabot-E	W32/Sdbot.worm.gen.bh	Win32 Worm
W32/Rbot-AAY		Win32 Worm
W32/Rbot-ACH	W32/Sdbot.worm.gen.bh	Win32 Worm

W32/Yaha.I@MM	I-Worm.Lentin.j W32.Yaha.L@mm W32/Lentin.L W32/Yerh.A Yaha.L!2095 Yaha.M Yerh	Win32 Worm
Whiter.F	Trj/Whiter.F	Trojan
Win32.Bropia.AQ		Win32 Worm
Win32.Lioten.MR		Win32 Worm
Win32.Mytob.CU		Win32 Worm
Win32.Propo		Win32 Worm
Win32.Puper Family		Win32 Worm
Win32.Rbot.CLW		Win32 Worm
Win32.Sober.O		Win32 Worm
Win32.Winshow.BM		Win32 Worm
Win32.Winshow.BV		Win32 Worm
Win32.Winshow.BW		Win32 Worm
WinCrash	Backdoor.WinCrash	Trojan
WORM_BROPIA.V		Win32 Worm
WORM_MUGLY.F	W32.Picrate.B@mm W32/Mugly Win32.Mugly.K	Win32 Worm
WORM_MYTOB.EK	W32/Mytob Win32.Mytob.CU	Win32 Worm
WORM_MYTOB.EQ		Win32 Worm
WORM_MYTOB.ER		Win32 Worm
WORM_OPANKI.G	W32/Opanki.worm	Win32 Worm
WORM_OPANKI.I		Win32 Worm
WORM_SEMAPI.A	Win32.Semapi.A	Win32 Worm
WORM_SOBER.U	W32/Sober Win32.Sober.O	Win32 Worm
Yaha.E	I-Worm.Lentin.G Lentin Lentin.G W32/Lentin.F@mm Yaha	Win32 Worm
Yaha.K	I-Worm.Lentin.h W32/Lentin.H@mm Yaha.K!e2a2 Yaha.M	Win32 Worm

[back to top]

Last updated May 18, 2005